Holistic Security and Risk Intelligence: Are Current Risk Management Methods Leading to Breach?

Christopher S. Middleton, Harsha Kalutarage, M. Omar Al-Kadri, Hatem Ahriz

***Abstract*—How could we better prepare industry and governments against holistic, hybrid, or second-order attacks?**

In this article we discuss the importance of addressing systemic and systematic risk management problems to provide holistic risk management and direct advances in technical security.

***Index Terms*—Holistic Security, Information Security, Cyber Security, Risk Management, Risk Intelligence, Hybrid Risk, Holistic Risk, Solarwinds.**

I. Introduction

BREACHES of Information Security (IS) such as the Solarwinds attack [1], are still frequently reported, with seemingly no organisation or government immune to breach.

Holistic or hybrid attacks are those which use a combination of people, physical and technical methods to overcome security, such as social engineering and phishing. Second order attacks such as Solarwinds, utilise a third party supply chain, hardware or software vendor to breach defences.

These types of attack are still common despite a significant body of research and the practical application of data science, to the prevention of breaches, such as Machine Learning (ML) classification of network traffic or email, and Artificial Intelligence (AI) enabled intrusion detection and prevention.

Regarding the Solarwinds attack which utilised the Solarwinds software to breach defences of industry and government, the IEEE Security and Privacy Editorial Board discuss perspectives [1]. Possible root causes include; Solarwinds cost cutting, lack of source code provenance, and a lack of software company accountability. However, despite correctly suggesting political and technical remediation, there was no discussion of risk management, or the inability of risk management systems to identify such risks and therefore direct technical security.

To establish if there is a potential gap in research, a brief survey of paper volumes on IEEE was undertaken, and is summarised in table I, for both all dates, and 2016 up until July 2021. The results suggest a significant body of research for technical security application, and a smaller body of research for holistic security, risk intelligence, and machine learning or artificial intelligence application to risk. This may suggest a disequilibrium in research, despite the International Organisation for Standardisation ISO 27001/2 management and code of practice requiring a holistic approach, with management of both technical and non-technical risks [2].

C. Middleton was with the Department of Computing at Robert Gordon University, Aberdeen, Scotland, UK, 2021. E-mail: c.middleton@rgu.ac.uk

Manuscript received December 2021; not revised

Metadata Search Terms	All Dates	2016 to Date
Machine Learning Intrusion Security	1926	1255
Machine Learning Detection Security	5199	3885
Artificial Intelligence Intrusion Security	2138	1373
Artificial Intelligence Detection Security	6276	4644
Subtotal	15539	11157
Information Security Risk Holistic	84	41
Information Security Risk Intelligence	994	624
Machine Learning Security Risk	643	489
Artificial Intelligence Security Risk	1107	799
Subtotal	2828	1953

TABLE I: Search Results from IEEE

A. A lack of discussion?

While the use of forensics is advised and frequently practiced for identifying technical causes, the impacts of a breach include organisation reputation, responsibility, and potential liability. These impacts can be existential and public relations spin is advised for managing them [3]. As risk management failings are highly sensitive to any organisation it can be suggested that there is little incentive to share risk management failings, for the benefit of others.

With this apparent conflict of interest, and a lack of reliable data on risk management failure, it is understandable that management surveys and articles often omit discussion of risk management as a root cause of breaches.

However, unlike technical vulnerabilities or perpetrators, which are often implicated as causes of breaches, we argue that a failure to identify specific risks could be a root cause of why many vulnerabilities remain unmitigated and open for exploitation. Breaches could instead be resultant of failures in risk management.

What can be objectively stated, is that any organisation's risk response is directed by its risk management, that technical security alone is not prime in reducing vulnerability to holistic attacks, and that to be effective at directing technical and non-technical countermeasures against holistic attacks, a risk management system should itself be holistic.

As such, it is necessary to objectively establish if risk management practices are efficient and effective in accurately representing holistic risk, and protecting against attacks like Solarwinds.

In this article we analyse systemic issues with whole risk management approaches and systematic issues with specific

methods of risk management. Where we identify significant problems, we also discuss how these issues could be addressed. We rely on academic literature and grey literature to support domain experience, which includes risk management, information security and business continuity.

II. Risk Information Systems and Siloes

Within a typical organisation there will be multiple systems recording risk information. These can be systems which formally perform a risk management role, technical systems performing a risk mitigation role, or other systems which incidentally contain useful risk information. We examine these different types of risk information systems and suggest they are siloed. Figure 1 illustrates typical holistic risk management and how the information is segmented by different stakeholders and disciplines.

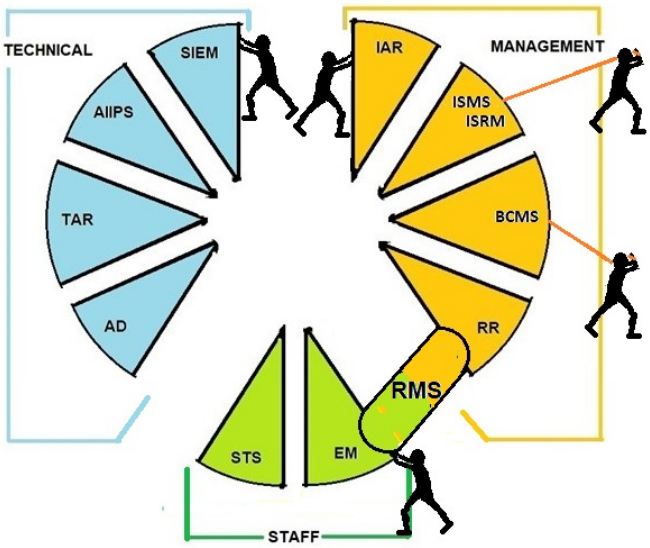

Fig. 1: Risk Information System Segments

The specification of management systems is described by standards of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). Of the formal management systems, the three types are most relevant to holistic risk management; information security, risk management, and business continuity; these may be managed by individual managers or teams within respective disciplines. These are described as follows:

ISO 27001/2 Information Security Management and Code of Practice - Concerned with the Confidentiality, Integrity and Availability (CIA) of information and information systems, ISO 27001 defines the establishment and review of information security management processes, and is complemented by the ISO 27002 security controls. The standards are abstract, but they are comprehensive and address both technical and non-technical security controls in approximately equal measure [2].

Information Security Management System (ISMS) – concerned with managing the information security program as a whole, the ISMS represents a store of parent security program risks, which can help prioritise program work, giving priority and status.

Information Asset Register (IAR) - the IAR is a part of an asset inventory within clause 8 of ISO 27001 [2]. It is an information centric system which records information assets; systems and applications used for the processing or storing of data.

ISO 27005 - Information Security Risk Management (ISRM) - addresses the assessment of information [security] risk. The standard specifies the iterative management processes involved in risk assessment including treatment by one of 4 actions, Tolerate (retain), Treat (modify), Transfer (share), or Terminate (avoid). The implementation of an ISRM system requires an emphasis on the ISO27002 annex of controls [2].

ISO 31000 - Risk Management - this standard is distinct from ISO 27005 in that it addresses organisation risk and not just information [security] related risk. The implementation of a Risk Management System (RMS) also referred to as Enterprise Risk Management (ERM), is concerned with identifying, assessing, and mitigating risks to people, locations and assets [2]. We suggest that an RMS typically contains a risk register (RR) for management of organisation risks and an event management module (EM) for staff to report incidents.

ISO 27031 and 22301 - Business Continuity Management - details a business continuity program, including strategy, planning, maintenance and specification of the Business Continuity Management System (BCMS). ISO 27031 addresses business continuity within an Information Security Management System (ISMS) scope, and ISO 22301 addresses business continuity for the whole organisation. Assessments conducted as part of the BCM program are essential for understanding organisation risk appetite [2]. The implementation of a BCMS includes Business Impact Analysis (BIA), risk assessment, and Business Continuity Plans (BCP).

Of multiple technical systems performing a risk mitigation role the Intrusion Prevention System, the Security Information and Event Management, and Technical Asset Register contain the most significant risk information. These systems would typically be managed within an IT department.

Intrusion Prevention System (IPS) - the security of network services is described within clause 13 of ISO 27001 [2]. Intrusion detection systems (IDS) are passively alerting and prevention systems (IPS) are actively preventing. AI enabled IPS systems collect data directly from a number of network devices and key IT infrastructure, using a combination of machine learning algorithms to map relationships and perform content inspection, with AI used in behavioral analysis and decision making.

Security Information and Event Management (SIEM) - the logging and monitoring of security events is described at various points within clauses 9, 10 and 12 of ISO 27001 [2]. A SIEM combines event management, logging and information management, collecting security events from diverse sources. The SIEM processes the data by; normalising, performing forensic analysis, and correlating events to identify malicious activities in real time.

Technical Asset Register (TAR) - the technical asset register, also known as the IT asset register or vulnerability management is specifically described in clause 12, and is part of an asset inventory within ISO 27001 [2]. It differs significantly from the IAR in that it is technology centric and stores information on; patch levels, location and custodian, not what information is stored on assets. These systems often integrate with vendor agent software and are capable of identifying some technical threats.

There are other systems which are not performing a risk management or risk mitigation role. However, they do contain useful risk information.

Support Ticket System (STS) - the STS, also known as the issue tracking system (ITS) or help desk software has three core components: ticket management, automation, and reporting. The STS manages the reporting of technical problems and jobs, including upgrades and faults. Although the STS is not specifically described in ISO 27001, the fault patterns and frequency information from the STS are potentially useful to holistic risk management, and it does contribute to incident management, clause 16 of ISO 27001 [2].

User Access Control (Windows Active Directory, AD) – The windows active directory stores information on windows IT assets along with users and stakeholders having access to these assets. Relational asset information, such as topology and access control information is already utilised by SIEM and IPS systems, to identify assets and users.

A. Risk Information Siloes

Figure 1 illustrates the segmentation of risk information systems, comprising formal risk management systems defined by standards, technical risk mitigation systems including applied data science, staff oriented systems, including systems which contain useful risk information. While these systems do cover every aspect of risk, it can be suggested that there are siloes between different types of risk information systems. These can be between systems of the same type, or systems utilising different methods of enumerating risk. Technical systems are typically managed by IT departments, and organisation risk, business continuity and information asset systems are the responsibility of managers within respective disciplines. Active directory and the STS are not a risk management systems, however they do contain useful risk information.

With separation of duties between different disciplines and stakeholders, we suggest that risk management is not an integrated or holistic process. For example, it would be challenging for a technical manager to interpret the exact nuances of non-technical risks bearing on technical risks and vice versa. More specifically, where risk systems are siloed between stakeholders and disciplines, the relationships between different types of risk will be poorly represented, and it is likely to create specific challenges for the implementation of holistic risk management in practice. In particular:

- **All Risk** - will information [security] risk response (ISMS/ISRM) coordinate with the organisation risk response (RMS)? For example, changing practice in regards to a non-technical attack vector, could result in a technical breach and vice versa.
- **Continuity** - will the organisation priority of continuity as defined in the BCMS be appropriately weighted against information security measures of confidentiality, integrity and availability? For example, prioritising CIA may impact business continuity, and prioritising business continuity may lead to a CIA breach.
- **Undesired Consequences** - whether technical risk is given non-technical risk context, for the avoidance on undesired consequences. For example, complex password policy resulting in passwords being written on paper.
- **Dynamic Risk** - whether is is possible to have reliable dynamic asset information and mapping of risk relationships, used to identify specific asset risks. For example, sensitive data on a laptop being moved to a less secure location.
- **Second Order Risks** - are risks to and from stakeholders and third parties external to the organisation accurately represented? For example, in the Solarwinds attack the third party software was the attack vector.

We suggest that having a number of systems covering the whole scope of information security risk management does not provide a holistic risk management system. However, having multiple discrete systems and managers acting to bridge system gaps is currently the only option available.

A holistic risk management system could produce dynamic and accurate risk assessment which meets the organisation's priorities and risk appetite. However, it may be necessary to remove reliance on human managers acting to bridge system gaps, and require fusion of information from formal risk management, technical risk mitigation and other systems containing useful security context. Data in staff systems, risk management systems and technical risk mitigation systems are distinctly different, but fusion of these data sets is required if a risk model is to accurately represent holistic risk. To dynamically assess risks may require application of multiple data science methods such as sentiment analysis, classification and AI decision making to interpret meaning from different data types, and relationships between technical risks and non-technical risks. Once there is fusion the risk relationships can be considered.

III. Errors Within Risk Management

Within technical security type II underestimation errors (or false negative) are considered less desirable than a type I overestimation error (or false positive) as they may result in non detection and breach. Many risk systems will also bias to a type I error, overestimation of risk, false positive and a waste of resources [4]. However, within the context of risk management there are two observations that can be made. The first is that all organisations have finite risk mitigation budgets and if the majority pick and choose which risks to mitigate, then a type I error is less desirable as a waste resources would result in less genuine risk being addressed overall than a type II error, underestimation of risk. The second observation is that for risk management, type I and type II errors are in large part resultant errors where more detailed examination of errors is required to establish root causes. Figure 2 shows the various types of experimental errors which can contribute to resultant type I and type II errors within risk management.

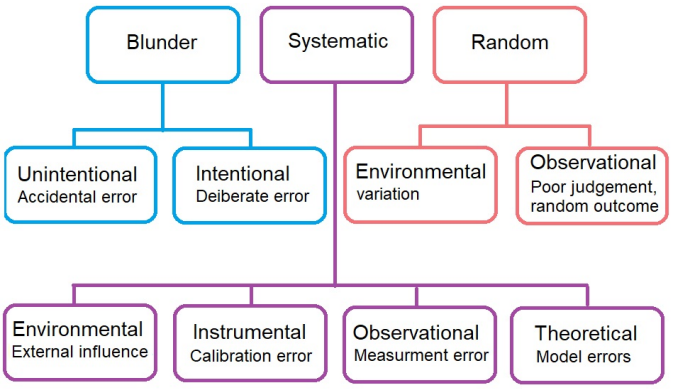

Fig. 2: Types of Experimental Error

We suggest that within the context of information security risk management, the following error conditions can be routinely observed:

1) **Systematic Observation Error** - Without sufficient training, users may lack understanding of the meaning of the values on scales and can often confuse terms; threats, likelihood, impact, and risk. This includes likelihood or impact values being considered as risk by the user without consideration of relative likelihood or impact. It can be suggested that a correct impact value may be entered with an incorrect likelihood value, or vice versa.

2) **Systematic Theoretical Simplification Error** - Models which simplify and interpret complex models are useful for humans, but they can lead to faulty judgments known as cognitive biases [5]. It is suggested that as holistic risk is a complex system, simplification to address the semantic gap is a cause of simplification error.

3) **Systematic Theoretical Approximation Error** - This is where approximation of multiple values in a formula leads to an incorrect calculation. With many current standards for qualitative risk management relying on integer values such as a scale of 1-5 to classify likelihood and impact, it can confidently be stated that significant approximation errors exist within risk management models.

4) **Unintentional Blunder Errors** - Human mistakes including; negligence, inexperience, lack of management, and lack of attention are the leading cause of errors in risk management. In a survey of GFSI (Global Financial Services Industry) it was confirmed that 86 percent of errors were attributed to human error [6].

5) **Intentional Blunder Errors** - There are multiple circumstances where intentional blunder errors may result from shortcuts taken or creation of values. We also suggest that there is a significant cohort of users of risk management systems who increase or reduce values to achieve a desired outcome. We suggest that these two groups can be described as:

- **Fallout phobic** - the understating of risk to avoid drawing attention or negative consequences.
- **Budget chasers** - the overstating of risk to secure budget or positive consequences.

To address the various errors in risk management, a much stronger emphasis should be placed on the design of models to specifically eliminate or minimise these experimental errors at source, rather than focus on type I and type II errors - which serve to confirm a [bad] model works as expected. As all of these errors also result from human interpretation of risk, through model simplification, or risk approximation to address the semantic gap, risk systems could reduce human interpretation, thus allowing more complex risk modelling at the back end. However, this will require human managers to cede some control, as complex risk models will require interpretation by data science techniques, with humans involved in inputs and then only interpreting holistic outputs.

IV. Problems Enumerating Security Risk

As holistic risk management includes the wider organisation risk, examples of wider risk enumeration problems can provide some insight. Professor Niall Ferguson examines historical exposure to risk from single assessment methods [7]. It is suggested that in 2008, worldwide financial risk management had excessive reliance on quantitative modelling and lacked qualitative context, which contributed to the disastrous financial crash. Prior and during this period, national security risk management in the US relied heavily on qualitative assessment, and lacked quantitative measurement of risk. This created opportunities for blunder errors, with poor consideration of consequences [7].

Returning to the information security domain, most organisations rely predominantly on either qualitative or quantitative measurement for their non-technical risk management, while technical risk is typically assessed via quantitative means alone [8].

It is suggested that the gap between theory and practice is causing routine failure in information security. In particular, quantitative risk analysis can be inaccurate due to the number of variables, or inclusion of variables which are difficult to accurately measure. Likewise, within qualitative risk assessment there is an inability to precisely estimate likelihood and impact. As such it is suggested that a mixed method approach is more appropriate for information security risk management [4].

Four types of risk assessment are defined as Qualitative, Semi-Quantitative (mixed – half and half), Quantitative, and a forth type called Transitional, which is mostly quantitative with some qualitative [8]. We suggest that this simplification does not consider that single assessment methods may be wholly unsuited to assessing risk. We further suggest that while the definitions of quantitative and qualitative are clear, the semi-quantitative and transitional methods could be confused. What can be stated is that mixed method enumeration of risk has many possible methods and understanding the goals and purpose of mixed method assessment will help identify the correct method.

A potential insight for mixed method assessment comes from the UK's National Cyber Security Centre (NCSC) discussion of assessment methods and their method for identifying which systems contain useful risk information [9]. NCSC describes how risk information should be classified on a 2 x 2 matrix; qualitative and quantitative, and either objective or subjective information, to establish where there is risk information bias within the organisation, referred to as 'Common organisational bias'. The aim is to avoid making risk decisions based on solely one method of enumeration, or one perspective. For example, quantitative and subjective data may be accurate, but it may lack the context that qualitative and objective data provides. The NCSC guidance does not suggest what a good mix or balance is, but it does highlight that empty spaces represent gaps in knowledge and understanding. The key takeaway from this method is the context which qualitative data can add to accurate quantitative data.

In consideration of [4], [7]–[9], we suggest describing 4 methods of quantifying security risk as follows:

1) **Qualitative** - the use of nouns or simple numeric scales to categorise risk. Such as rare likelihood, major impact, or 1-5 for likelihood and impact along with a 5 by 5 matrix for risk.
2) **Quantitative** - numeric measurement applied to a formula, such as Annual Rate of Occurrence (ARO), Single Loss Expectancy (SLE), Annual Loss Expectancy (ALE).
3) **Mixed** - converting qualitative measures to numerical values and combining with quantitative measurements in more complex numerical formulas. this allows the use of more detailed numeric scales, such as 1 to 100, or 0.0 to 10.0, and charts to plot clusters of risk. Numerous scales are applied in a formula, such as in the Common Vulnerability Scoring system (CVSS)
4) **Hybrid** - again combining a mix of quantitative and qualitative data. However, instead of both being applied in a more complex formula, quantitative data is used where it is known to be accurate and qualitative data is then applied to give context, dimension and define relationships. We suggest this method is inherently more complex and suited to AI decision making. The hybrid method can be further categorised as:

- **Explanatory sequential** - where quantitative data then qualitative data are analysed sequentially.
- **Exploratory sequential** - where qualitative then quantitative data are analysed sequentially.
- **Embedded** - where both methods are analysed simultaneously.

We suggest that holistic risk is defined by both measurable factors and organisation context and therefore cannot be represented by quantitative or qualitative assessment alone. In consideration of [4], [7]–[9], we further suggest that risk systems which are holistic should utilise quantitative data due to its accuracy and precision, but qualitative measurement should be used to give context to this data. Contexts, could include the relationships between different ontology objects and elements, such as assets, stakeholders, and topology.

V. Are Current Risk Models Holistic?

Each organisation's risk appetite is different, as are the individual models and controls chosen. While organisations may struggle to mitigate risk cost effectively, it is suggested that whatever risk methods are used, a focus on data collection and preparation is essential to ensure the quality of information before conducting risk assessment [10].

For a risk management framework to be considered holistic, we suggest that the following should be considered:

- **Approach** - frameworks which have demonstrable technical method and are not limited to only guidelines or abstract methodology, which could lead to observation, approximation and blunder errors due to interpretation from the end user.
- **Enumeration** - we have suggested that single methods of assessment (quantitative, qualitative) may not be suited to holistic risk and frameworks with a mixed or hybrid assessment method are more suited.
- **Complexity** - if a framework has low levels of complexity then it simplifies the reality of complex risk and is more likely subject to systematic theoretical simplification error.
- **Priority** - given finite resources, risks of the same value could be prioritised according to business objectives. In addition to enumerating risk, frameworks should provide metrics for prioritising all risks, such as business continuity, effort to mitigate, or return on investment.
- **Scope** - frameworks should include management, operational and technical risk, in addition to managing

people and HR risk. Frameworks which predominantly address technical or non-technical aspects of security should not be considered holistic.

Table II gives a summary of the above information extracted from comparison of risk management frameworks [10]–[14]. The comparison of risk management models is dependent on the criteria used within reviews and several models have different versions or implementations suited to respective organisation size and resource. As such, there are some bands of values in table II which is intended as a guide. In addition, various insights for the different models are noted below:

1) **OCTAVE** - Operationally Critical Threat, Asset, and Vulnerability Evaluation. It is workshop based with software tools, and includes hardware, software, information, people, and systems as assets [12]. It is flexible and offers several methods tailored for specific organizations and contexts, where disparate processes can be carried out by small teams [13]. Quick and adaptable, its ontology is business process oriented and it minimises technical details, producing only organisation risk information [14]. However, it does not allow quantitative assessment [12] and is internal only, where it does not consider third parties [11].
2) **NIST SP 800** - National Institute of Standards and Technology. Suited to technological risk, being more tactical and operational. It includes security checklists, interviews and questionnaires. It also has some inclusion of third parties but crucially not human resources, or management aspects [11]. NIST is approved for use by government agencies and its focus is more physical assets. However, as NIST is not available with computer support for implementation, its method can be considered a guideline [12].
3) **MEHARI** - MEthod for Harmonized Analysis of RIsk. Is a mostly qualitative method, requiring input from managers and experts, while aligning to ISO 27002 controls [10] and for the implementation of ISO 27005 [13]. It allows some mixed quantitative and qualitative analysis within formulas and uses an extensive knowledge database, with audits carried out to identify new vulnerabilities [14]. However, implementation is somewhat inflexible, requiring dedicated software and a pre-defined knowledge base aligning to ISO 27002 controls. It also lacks a risk evaluation phase [13].
4) **ISO 27005** – International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). It is suited to management practices and its scope includes people, procedure, physical and technology risks [11]. It has an extensive taxonomy, conceptual model and Risk Management Framework, but only describes the Risk Assessment process at an abstract level [13]. Data is collected via interviews, questionnaires, process reviews, and work audits. It is further suggested that ISO27005 could be considered holistic as it requires documentation on all controls, but it is also abstract regards implementation having little in the way of practical method [11]. However, it cannot be used in isolation, and requires other risk assessment tools for implementation. With prescribed ISO 27002 controls it is also limited in its ability to identify new risks [13].
5) **CORAS** - Platform for Risk Analysis of Security Critical Systems. It is a quantitative method using the Unified Modelling Language (UML) to define ontology elements and to illustrate relationships between users and the environment [10]. Of medium complexity, it provides a model–based framework, and requires expert knowledge, but lacks a risk evaluation phase [13]. Some aspects can be abstract and require significant expertise and interpretation. It includes some definition of relationships and dependencies [10]. However, it is dependant on its own unique terminology for risk management, and it adopts the risk assessment methods of AS/NZS 4360 general risk management standard, which does not specialise in information security [15].
6) **EBIOS** - Expression des Besoins et Identification des Objectifs de Sécurité. Medium level of complexity, the methods are generic and can be applied to objects of various sizes and complexities [13]. It is further noted that this is a method based model which utilises self assessment and brainstorming in a multi-discipline work group [14]. It can be implemented by managers or operational staff but is not intended for technical staff or to provide technical risk detail [13].
7) **CRAMM** - Certified Counter-Intelligence Threat Analyst Risk Analysis and Management Method. Varying levels of complexity to suit the organisation [14]. The assessment process is mostly automated by software tools, but requires expert knowledge [13]. However, the method lacks detail on implementation and follow-up, including detail on training, meetings or workshops, monitoring or review of the effectiveness of controls, and improvement of management processes [15]. These omissions may affect the quality control of system implementation.

What can be stated is that with the exception of ISO 27005/2 and MEHARI, the models are limited by the scope of risks assessed. The majority of models either prescribe a single enumeration method or are abstract in allowing any, except MEHARI and CORAS, which allow for a limited mixed (but not hybrid) enumeration method. Model complexity is demonstrated in several methods, and with some having software supporting this. However, end users are encouraged to choose models based on skill set or resource, rather than the need to accurately represent holistic risk. Another concern is that the model comparisons do not compare modelling for relationships between technical and non-technical risk, which we suggest is necessary to reduce siloed risk.

Although ISO 27005 and ISO 27002 may have a relatively holistic scope, there are 2 significant limitations. The first is that ISO 27005 is abstract and does not prescribe methodology on how a holistic risk should be assessed in practice. The second limitation is that ISO 27005 is prescribed ISO

	OCTAVE	NIST SP 800	MEHARI	ISO 27002/5	CORAS(d)	EBIOS	CRAMM
Approach	Method	Method/Guide	Method	Abstract/Guide	Method/Guide	Method	Method
Enumeration	Qual	Any	Quant/Qual	Any	Quant/Qual	Qual	Qual
Complexity	Low/Med	Medium	High	Medium	Medium	High/Med	Low-High
Priority/Risk	Both	Risk	Risk	Both	Both	Risk	Risk
Scope	Mgt/Oper	Oper/Tech	Holistic	Holistic	Mgt/Oper	Mgt/Oper	Mgt/Oper/Tech
Limitations	Internal Only	Technical Bias	Flexibility	Method/Controls	Generic Risk	Limited Technical	Quality Control
References	[11], [12], [14]	[11], [12], [14]	[10], [12]–[14]	[11], [13], [14]	[10], [13], [15]	[13], [14]	[13]–[15]

TABLE II: Established Risk Model Comparison

27002 controls, and while these are comprehensive, it may be a disadvantage where there is need to identify new attack vectors.

It is suggested that if adopting the above methods, at least 2 different risk models may be required, 1 for technical assessment and 1 for non-technical or management aspects [11]. However, we would suggest that overlap and lack of fusion between two discrete methods would limit accurate enumeration of holistic risk.

While the implementation of ISO 27002/5 standards through MEHARI is comprehensive, it does not enumerate relationships in calculation of risk, has a high level of complexity with a 3000+ knowledge base, and may lack flexibility.

VI. Creating a Holistic Risk System

In consideration of the options for creation of a holistic risk management system, we suggest that a holistic risk management system will have inevitable complexity. The level of effort required to manage such a system by human management could make it unsuited to all but the largest and well resourced organisations. In addition, human or process driven holistic systems may require model simplification due to semantic gap issues, this may result in new errors and make the manual/human approach wholly unsuitable for holistic risk management systems.

As we have suggested that existing risk models are either non-holistic, and/or have significant limitations, combining them may result in a system with errors, omissions, bias, and either incorrectly weighted or absence of relationships between technical and non-technical risk. Likewise, basing an ML/AI implementation on a combination of existing models may be subject to similar problems, as the underlying model remains deficient. Instead, we suggest that the current ISO standards could be utilised as a reference for holistic risk management, but that new holistic risk management models are required. These could incorporate technical and risk management information, along with non-risk organisation context, in order to establish relationships for dynamic risk assessment. We suggest this may prove more suited to identifying and accurately enumerating holistic or second order attacks.

However, creating holistic risk models requires a number of model and technical challenges to be addressed. These include:

Errors in Risk Management - a foremost consideration is a design process which eliminates or minimises experimental errors in risk models. In addition, when the model is applied in practice, the use of good human interface design, could mitigate new systematic errors being introduced.

Hybrid Risk Enumeration Methods - to address qualitative guess work or over reliance on quantitative data without context, hybrid enumeration methods will need to allow the context of qualitative assessment to be applied to more accurate quantitative measurement of risk. Systems need to capture risks which can be either tangible or intangible.

Fusion of Risk Information Systems - for a model to be holistic it will require fusion of data from staff systems, risk management systems, technical systems, and other systems with organisation context. With these data sets being dissimilar, several data algorithms will be required to solve different problems, potentially; machine learning classification, content inspection, sentiment analysis, and the mapping of relationships.

Ontology Selection - to address omissions in existing risk model ontologies, we suggest careful selection of new top level ontology elements, which can represent an organisation and its security risk. We suggest that there are [at minimum] six ontological elements which are critical to representing an organisation and its security risk, these are: assets, stakeholders, topology, financial metrics, attack vectors and mitigation.

Ontology Relationships - risk modelling may require significant complexity in relationships, where this is intended to be interpreted by ML/AI at the back end, rather than human managers. If each element is assigned initial domain expert qualitative values for likelihood, impact, and risk, the inclusion of qualitative relationships defined by the correlation of Continuity (business criticality), Confidentiality, Integrity and Availability (CCIA) metrics may be key to having a risk model which is a dynamic representation of holistic security risk. A conceptual example is illustrated in figure 3.

Dynamic Risk Interpretation - after all the data is processed and fused into a smaller number of data sets, it may require interpretation by artificial intelligence, trained by either supervised learning or reinforcement learning for decision making. It is the decision information that we suggest could be used to inform risk managers.

Development of Holistic Risk Data Set - To test new holistic risk models, a holistic risk management benchmark

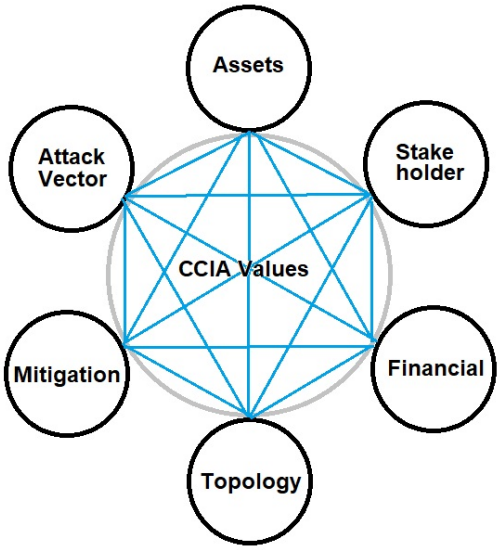

Fig. 3: Suggested Conceptual Ontology Relationships

data set may be required. Such a data set could include corresponding data from; technical risk mitigation systems, non-technical risk management systems, and other systems containing useful risk context information. This could support the research and development of holistic risk models utilising ML and AI.

Closing Remarks - The Solarwinds attack [1] and Professor Niall Ferguson's macro examination of risk management failure [7] highlight the imperative of future work to improve risk management. We have suggested that the narrative of perpetrators and technical security being root causes is incorrect, as the attackers have simply identified a weakness and exploited it. With organisations having disincentive to disclose risk management failings [3], it can be suggested there is an absence of reflection and remedy of risk management failure across governments and large organisations. It can be further suggested that holistic attacks will continue to be highly successful until risk management is able to address complex and dynamic relationships between all the elements in a security ontology. Such a system could ultimately assist decision makers in all types of organisation.

ACKNOWLEDGMENTS

This work is being conducted as a PhD research project at Robert Gordon University, UK. It is privately supported by Wee Group Ltd.

Christopher S. Middleton (2021) is an experienced security professional, with a 20-year career in computing, business continuity, risk management and information security. He is currently undertaking a PhD at Robert Gordon University, UK – Holistic Information Security Risk Management Aided by Artificial Intelligence. He received an MSc in Cyber Security (distinction) from Robert Gordon University, UK, in 2020, with a prior thesis of [high dimension] Information Security Risk Profiling Aided by Machine Learning.

Dr Harsha Kalutarage is a lecturer in Cyber security at Robert Gordon University, UK, holding a PhD in Computing (Cybersecurity). His research in Security focuses on AI techniques protecting AI-embedded systems. Harsha has 10+ years of research experience, 50+ publications, with patent and technology transfers to industry. He has served as an invited speaker, guest editor, technical co-chair and PC member for numerous venues. Before RGU, he was a Senior Research Engineer at Queen's University Belfast and researcher at Coventry University.

M. Omar Al-Kadri (2021) received his B.Eng. in Computer Engineering from IUST, Syria, in 2010, M.Sc. (distinction) in Networking and Data communication from Kingston University, UK in 2013, and Ph.D in Informatics and Telecommunication engineering from Kings College London, UK, in 2017. He is currently a senior lecturer in Cyber Security at Birmingham City University. His research includes security of healthcare wireless communications, security of vehicular networks, security of IoT, full-duplex communications, and risk management.

Dr Hatem Ahriz is a senior lecturer with 20 years' experience in academia. He currently leads the masters degree program for cyber security at Robert Gordon University with research interest in the application of AI to security. He holds ISACA's CISM certification.

REFERENCES

[1] Sean Peisert, Bruce Schneier, Hamed Okhravi, Fabio Massacci, Terry Benzel, Carl Landwehr, Mohammad Mannan, Jelena Mirkovic, Atul Prakash, and James Bret Michael. Perspectives on the solarwinds incident. *IEEE Security Privacy*, 19(2):7–13, 2021.

[2] it governance uk. iso 27000 series of standards. https://www.itgovernance.co.uk/iso27000-family, 2018.

[3] Paul Cerrato. Chapter 10 - preparing for and coping with a data breach. In Paul Cerrato, editor, *Protecting Patient Information*, pages 125–132. Syngress, Boston, 2016.

[4] R. Oppliger. Quantitative risk analysis in information security management: A modern fairy tale. *IEEE Security Privacy*, 13(6):18–21, Nov 2015.

[5] R. J. Heuer. *Psychology of intelligence analysis*, pages 111–114. Center for the Study of Intelligence, Central Intelligence Agency, 1999.

[6] Seema Sharma and Babu Ram. Causes of human errors in early risk assesment in software project management. In *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*, ICTCS '16, New York, NY, USA, 2016. Association for Computing Machinery.

[7] Naill Ferguson. Applying history in real time: a tale of two crises. https://www.youtube.com/watch?v=LeWZ8hw7Yr0, Oct 2018.

[8] Luke Jasper. qualitative-vs-quantitative-which-approach-risk-right. https://www.linkedin.com/pulse/qualitative-vs-quantitative-which-approach-risk-right-luke/, 2021.

[9] NCSC. Risk information guidance - variety in risk information. https://www.ncsc.gov.uk/collection/risk-management-collection/essential-topics/variety-risk-information, 2021.

[10] C. Fakrane and B. Regragui. Interactions and comparison of it risk analysis methods. In *2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech)*, pages 1–7, 2018.

[11] Anuj Tewari. comparison between iso 27005, octave and nist sp 800-30-2013. https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30, Sep 2013.

[12] Umesh Kumar Singh and Chanchala Joshi. Comparative study of information security risk assessment frameworks. *International Journal of Computer Application*, 2(8):2250–1797, Jan 2018.

[13] Dan Ionita. Current established risk assessment methodologies and tools. *Affiliation: Centre for Telematics and Information Technology, University of Twente*, Feb 2014.

[14] Filipe Macedo and Miguel da Silva. A comparative study of risk assessment methodologies for information systems. *Bulletin of Electrical Engineering and Informatics*, 1(2), 2012.

[15] K Srujan and M Rao. Enterprise information security risk management. pages 20–24. Computer Society of India, 2017.